Région académique
DANE
Délégation Académique au Numérique Éducatif

Vademecum
pour la mise en place du RGPD dans les EPLE

1. Qu'est-ce que le RGPD ?

Le Règlement général sur la protection des données (RGPD) est le nouveau cadre juridique de l'Union européenne qui gouverne la collecte et le traitement des données à caractère personnel. Il a pour objectifs de :

- Donner aux citoyens de l'Union Européenne plus de visibilité et de contrôle sur leurs données à caractère personnel ;
- Permettre à « l'administration » de maîtriser le cycle de vie des données et de pouvoir les transmettre sur simple demande.

Le RGPD concerne les entreprises, les associations, les collectivités locales et toutes les entités du service public. Les services de l'éducation nationale ainsi que les écoles, collèges et lycées, les universités… doivent l'appliquer.

Le RGPD simplifie les démarches et responsabilise tous les acteurs : les déclarations auprès de la CNIL disparaissent et sont remplacées par l'obligation de documenter sa conformité (la CNIL conserve toutefois un droit de contrôle sur le respect de cette procédure et sur l'application de la loi).
Les écoles, les collèges et les lycées doivent être capables de garantir et de prouver que leurs traitements de données à caractère personnel sont conformes et sécurisés.

Les textes
La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles modifie la loi Informatique et Libertés du 6 janvier 1978 pour l'adapter au Règlement général sur la protection des données (RGPD) adopté par le Parlement européen le 25 mai 2018.

2. Qu'est-ce qu'un traitement de données à caractère personnel ?

Un traitement est une opération ou un ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Qu'est-ce qu'une donnée à caractère personnel ?

Est considérée comme « donnée à caractère personnel » toute information permettant de faire le lien directement ou indirectement avec une personne physique. Le texte ne précise pas le type de support (numérique ou papier) :
"*Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ». Concrètement, une donnée à caractère personnel peut être un nom, un prénom, une date de naissance, mais aussi un pseudonyme, un numéro de sécurité sociale, une plaque d'immatriculation de véhicule, un numéro de téléphone, une adresse IP, un historique de navigation, une géolocalisation, une photographie, un avatar…*"

3. Comment s'applique le RGPD selon les différents types de données à caractère personnel ?

Tout traitement de données concernant les élèves (résultats scolaires, professions des parents, revenus du foyer, pays de naissance, vaccinations, allergies si elles sont conséquentes en milieu scolaire…), parents ou personnels, doit dorénavant être inscrit sur un registre interne à l'école ou à l'établissement, et maintenu à jour.
La Loi Informatique et libertés du 6 janvier 1978 est ainsi modifiée, dans son article 8, par les lois du 14 mai 2018 et du 20 juin 2018 :
« *Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.* »
Ainsi les démarches déclaratives auprès de la CNIL restent obligatoires pour le traitement de données **dites sensibles**, comme par exemple les données biométriques (empreintes digitales pour le passage à la cantine) et les vidéos captées par des caméras dans l'enceinte de l'établissement. Sont également **sensibles** : l'appartenance syndicale d'un enseignant ou d'un parent à une association (quand elle n'est pas publique), le régime alimentaire s'il

révèle une religion (halal, casher…), la nature d'un handicap, d'une déficience ou d'une affection, un justificatif d'absence à caractère religieux (ramadan…).

Qu'en est-il des statistiques
Le secret statistique est également régi par l'obligation de conformité aux règles encadrant les traitements de données à caractère personnel (Secret statistique et protection des données – INSEE 2017). Il est interdit de publier des données qui permettraient une identification indirecte d'une personne ou même, sans pouvoir l'identifier, d'obtenir une information à son sujet.

4. Quels sont les droits des membres de la communauté scolaire ?

- Droit d'information : Toute personne a le droit de connaître les données collectées (qui la concernent) et la finalité de leur traitement.
- Consentement / Droit d'opposition : Toute personne a le droit de s'opposer au traitement de ses données à caractère personnel, ou de retirer son consentement à tout moment, pour des motifs légitimes, sauf si le traitement répond à une obligation d'intérêt public (éducation, santé…).
- Droit de rectification : Toute personne peut demander à corriger certaines informations la concernant.
- Protection des mineurs de moins de 15 ans : Lorsque le mineur est âgé de moins de 15 ans, le consentement au traitement doit être donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale, pour les traitements réalisés sur un(des) service(s) de la société de l'information (réseaux sociaux, Drives, blog, site Web…). Ce double consentement est exigé par la Loi « Informatique et libertés » du 14 mai 2018

La majorité numérique en France
La loi « Informatique et liberté » du 14 mai 2018 fixe l'âge de la majorité numérique à 15 ans en France : Un mineur peut consentir seul à un traitement de données à caractère personnel, à compter de l'âge de quinze ans. Il peut alors retirer son accord et demander l'effacement de ses données, sauf pour un traitement d'intérêt public (éducation, santé…).

- **Droit d'accès** : Toute personne peut accéder à l'ensemble des informations la concernant, et en obtenir une copie. Le responsable de traitement est tenu de répondre à cette demande dans un délai de deux mois.
- **Portabilité** : Les données recueillies doivent pouvoir être, à la demande de la personne concernée, restituées sous forme structurée, exportables et importables sur un service analogue. Ce droit ne s'applique pas au traitement nécessaire à une mission d'intérêt public (éducation, santé) ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement (traitement mis en œuvre par le ministère, un service académique, ou bien le chef d'établissement ou le DASEN dans l'exercice de leur fonction).
- **Réparation du préjudice** : Toute personne ayant subi des dommages matériels ou moraux du fait d'un traitement de données inadapté pourra demander réparation. Une association de protection des données, ou bien un groupe de parents, pourra entamer un recours collectif.
- **Droit à l'oubli** : Dès lors qu'une personne estime qu'une information affichée sur une plateforme ou par un moteur de recherche porte atteinte à sa réputation ou à sa vie privée, il peut demander à ce que cette information soit effacée de la plateforme ou des résultats du moteur de recherche (déréférencement).

5. Quelles sont les obligations à respecter dans le traitement des données à caractère personnel ?

Les traitements des données à caractère personnel doivent respecter les règles suivantes :

- **Transparence** : Le responsable de traitement doit informer, en des termes clairs et simples, aisément compréhensibles par les personnes concernées, de l'utilisation de leurs données à caractère personnel.
- **Licéité** : Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes :
    - La personne concernée, ou l'élève mineur (moins de 15 ans) et son responsable parental, a /ont consenti au traitement des données pour la(les) finalité(s) indiquée(s) ;
    - Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
    - Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (éducation, santé…).
- **Consentement** : Avant de procéder au recueil de données à caractère personnel, le responsable de traitement doit obtenir le consentement des personnes concernées. La preuve du consentement doit être matérialisée. Toutefois dans le cadre d'une mission d'intérêt public (éducation, santé…), le consentement parental n'est pas requis pour pouvoir collecter, traiter et conserver les données des élèves, dès lors que l'application utilisée est conforme au RGPD. Ainsi, si le traitement est mis en œuvre par le ministère, un service académique, ou bien le chef d'établissement ou le DASEN dans l'exercice de leur fonction, ce consentement n'est pas nécessaire sur les outils de gestion de la vie scolaire, sur le réseau pédagogique de l'école ou de l'établissement, sur l'ENT et ses différentes fonctionnalités (forums, groupes collaboratifs…).

L'offre directe de services de la société de l'information pour les mineurs de moins de 15 ans : La nécessité du « double consentement conjoint »
En ce qui concerne les traitements effectués sur un(des) service(s) de la société de l'information, la Loi Informatique et libertés du 14 mai 2018 exige :

- le consentement explicite des élèves de plus de 15 ans.
- le « *double consentement conjoint* » (élève – parents) pour les élèves de moins de 15 ans.

Les activités pédagogiques doivent respecter ce consentement ou double consentement si elles conduisent à un traitement de données à caractère personnel sur des réseaux sociaux, des Drives, blogs, sites Web, Webjournal, Webtélé, Webradio…

- **Limitation des finalités** : Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites, légitimes.
- **Minimisation des données** : Seules peuvent être collectées les données adéquates, pertinentes, et limitées à ce qui est nécessaire au regard des missions de l'établissement pour lesquelles elles sont traitées.
- **Sécurité et confidentialité** : Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident. Les serveurs doivent être protégés en lieu sûr, répliqués, et visibles seulement des personnes habilitées.
- **Durée de conservation** : Une durée maximale de conservation des données doit être définie. Cette durée varie selon les différents objectifs (en base active) et les éventuelles obligations légales de conservation. Une fois que l'objectif poursuivi par la collecte des données est atteint, celles-ci doivent être supprimées sur toute la chaîne de sauvegarde, ou bien archivées (en archivage administratif ou définitif), selon les règles les concernant.

6. Des questions à se poser

- Jusqu'à quand ai-je besoin de données à caractère personnel pour atteindre l'objectif fixé ?
- Ai-je des obligations légales de conservation de ces données pendant un certain temps ?
- Dois-je conserver certaines données à caractère personnel en vue de me protéger contre un éventuel contentieux ? Lesquelles ?
- Jusqu'à quand puis-je faire valoir ce recours en justice ?
- Quelles sont les règles de suppression et/ou d'archivage (durée) de ces données à caractère personnel ?

A. Qui est le responsable de traitement des données ?

Le responsable du traitement est « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ». Il s'agit de la personne qui détermine la réponse aux questions suivantes :

- A quoi va servir le traitement ?
- Comment l'objectif fixé sera atteint ?

Pour les applications nationales et académiques, le responsable de traitement est :

- Au niveau ministériel : le ministre (directeurs par délégation).
- Au niveau académique : le recteur, ou les chefs de service rectoraux et DASEN par délégation.
- Au niveau d'un EPLE : le chef d'établissement.
- Au niveau d'une école primaire : le DASEN (ni les directeurs d'école, ni les IEN n'ont le statut de personne morale).
- Pour l'enseignement privé sous contrat avec l'état : le directeur de l'établissement.

B. Les traitements effectués par les enseignants

Tous les traitements réalisés sur les outils de l'école, du collège ou du lycée – ou fournis par l'établissement - (ordinateur, clé USB, ENT…), ou/et partagés dans le cadre du travail, doivent figurer sur le registre de l'établissement. Les professeurs ne peuvent se retrancher derrière leur liberté pédagogique et doivent être transparents à l'égard du responsable des traitements de l'établissement.
Certains outils utilisés par les enseignants, dans le cadre de leur liberté pédagogique, peuvent conduire à un traitement de données personnelles de leurs élèves (adresses internet utilisées pour s'inscrire à certains services…) à reporter sur le registre de l'école ou de l'établissement. De même, un professeur qui transmet à une plateforme de travail collaboratif (de type Pad hors ENT par exemple) ou par un système de communication (Skype, MSN, Hangout…) des données d'élèves, doit en informer le responsable des traitements pour renseigner le registre. Des listes de notes ou de compétences et des données récoltées auprès de parents, stockées sur un support, même personnel, constituent également un traitement à répertorier, de manière générique, dans le registre.

C. Les risques en cas de manquement éventuel au RGPD

Le responsable du traitement peut encourir un risque de sanction (CNIL, administrative ou pénale) en cas de non-respect du RGPD (formalités préalables…).
Les amendes ne sont pas applicables aux traitements mis en œuvre par l'État et ses services déconcentrés, ou par les chefs d'établissement et DASEN lorsqu'ils mettent en œuvre un traitement au nom de l'État ou en qualité de représentant de l'État. La CNIL n'a pas tranché, en cas de traitement au nom de l'EPLE ou de l'école, mais les chefs d'établissements et DASEN seront protégés.
Le chef d'établissement ne peut être tenu pour responsable d'un défaut de protection des données dans un traitement personnel effectué par un enseignant, s'il n'en avait pas connaissance.

D. Que faire en cas de violation de données à caractère personnel ?

La violation de données à caractère personnel doit être communiquée par le responsable de traitement :

- à l'autorité de contrôle, la CNIL, dans un délai de 72 heures (week-end compris) après en avoir pris connaissance. Si ce délai est dépassé avec un risque pour les droits et libertés des personnes, la notification doit être accompagnée des motifs du retard ;
- à chaque personne concernée dans les meilleurs délais.

Le responsable de traitement coopère alors avec les représentants de la CNIL, à la demande de celle-ci.

7. Quelles sont les précautions à prendre en cas de sous-traitance ?

Lorsque le responsable du traitement fait appel à des sous-traitants ou des prestataires, il doit s'assurer que ces derniers présentent des garanties suffisantes de mise en œuvre des mesures techniques et organisationnelles appropriées, de manière à ce que chaque traitement réponde aux exigences du RGPD.

« *Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement.* » Le contrat, ou l'autre acte juridique, se présente sous une forme écrite, y compris en format électronique. L'application, par un sous-traitant ou d'un prestataire, d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir d'élément pour démontrer l'existence des garanties suffisantes.
« *Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.*
Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données sont imposées à cet autre sous-traitant. Lorsque ce dernier ne remplit pas ses obligations, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations ».
Les sous-traitants proposant des logiciels de vie scolaire possèdent souvent eux-mêmes des sous-traitants (hébergement des données…). Le responsable de traitement a intérêt de demander au sous-traitant la cartographie de la circulation des données.

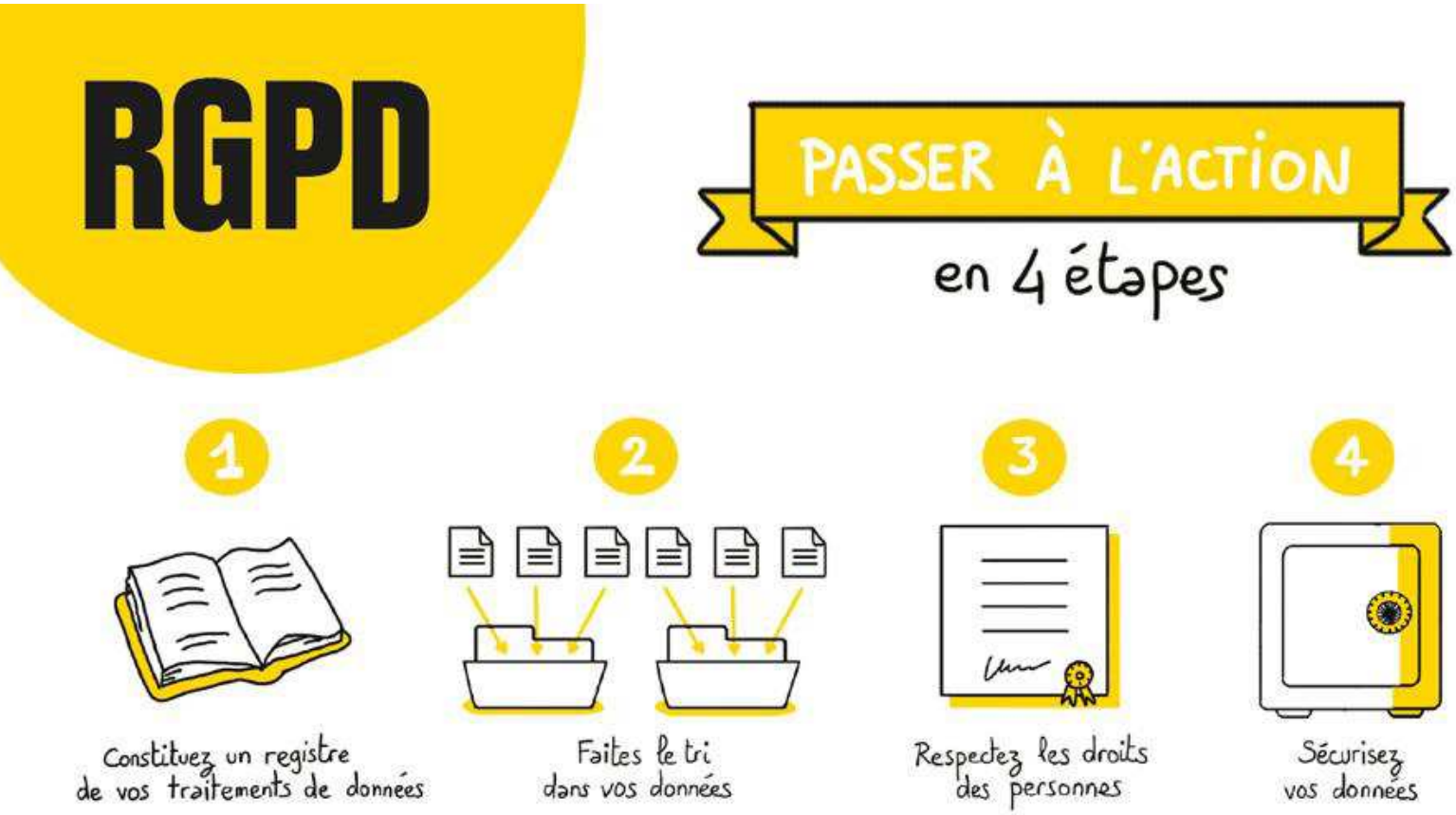
A. Quel est le contenu du contrat ou d'un autre acte juridique avec le sous-traitant ou le prestataire ?

Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant ou le prestataire :

- ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
- veille à ce que les personnes autorisées à traiter les données à caractère personnel soient soumises à une obligation de confidentialité ;
- prend toutes les mesures requises en matière de sécurité du traitement des données ;
- respecte les conditions requises pour recruter un autre sous-traitant ;
- aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, à donner suite aux demandes éventuelles des personnes concernées ;
- aide le responsable du traitement à garantir la sécurité, compte tenu de la nature du traitement et des risques ;
- selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation de ces données ;
- met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations et pour permettre la réalisation d'audits ou d'inspections par le responsable du traitement ou un autre auditeur qu'il a mandaté.

Certains sous-traitants s'inscrivent déjà dans une logique de mise en conformité :
- L'éditeur de logiciels Index Education met à disposition sur son site une FAQ qui répond à l'essentiel des questions. Il propose également une fiche pré-remplie à compléter et à ajouter au registre de traitement de l'établissement.
- l'opérateur Canopé met également à disposition une FAQ et des fiches de traitement pour les solutions documentaire BCDI et eSIdoc qu'utilisent la plupart des CDI.

8. La mise place du RGPD en 4 étapes



1ère étape	A. Constituer un registre de vos traitements de données

Le registre de traitement de vos traitements de données vous permet de recenser tous vos fichiers et d'avoir une vue d'ensemble. Il est prévu par l'article 30 du RGPD et participe à la documentation de la conformité

Il faut avant tout identifier toutes les activités administratives et pédagogique de l'établissement qui nécessitent la collecte et le traitement de données. Le registre doit permettre d'identifier précisément :

1. le cas échéant, le nom et les coordonnées du responsable conjoint du traitement mis en œuvre
2. les finalités du traitement, l'objectif en vue duquel vous avez collecté ces données
3. les catégories de personnes concernées (client, prospect, employé, etc.)
4. les catégories de données personnelles (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, données de localisation, etc.)
5. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants auxquels vous recourez
6. les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
7. les délais prévus pour l'effacement des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut les critères permettant de la déterminer
8. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles que vous mettez en œuvre

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de votre conformité au RGPD. Il vous permet de documenter vos traitements de données et de vous poser les bonnes questions : ai-je vraiment besoin de cette donnée dans le cadre de mon traitement ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle vous permettra d'en déduire un plan d'action de mise en conformité de vos traitements aux règles de protection des données.
La CNIL présente dans cet article les éléments essentiels relatifs au registre et propose également un modèle de base répondant aux conditions posées par le RGPD.

2ème étape	B. Faites le tri dans vos données

La constitution du registre vous permet de vous interroger sur les données dont votre établissement a réellement besoin.

Pour chaque fiche de registre créée, vérifiez que :

- les données que vous traitez sont nécessaires à vos activités ;
- vous ne traitez aucune donnée dite « sensible ». Si vous en traité, vérifiez que vous en avez bien le droit de les traiter ;
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

A cette occasion, améliorez vos pratiques ! Minimisez la collecte de données, en éliminant de vos formulaires de collecte et vos bases de données toutes les informations inutiles. Redéfinissez qui doit pouvoir accéder à quelles données dans votre établissement. Pensez à poser des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans vos applications.

3ème étape	C. Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (élèves, parents d'élèves, enseignants, etc.).

Informez les personnes
A chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.
Vérifiez que l'information comporte les éléments suivants :

- pourquoi vous collectez les données (« la finalité » ; par exemple pour permettre aux élèves de manger à la cantine) ;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime », pour des traitement administratifs ou pédagogiques) ;
- qui a accès aux données (indiquez des catégories : les personnels de direction, un prestataire, etc.) ;
- combien de temps vous les conservez (exemple : « 5 ans après la fin de la scolarité ») ;
- les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Appuyez-vous sur les exemples de mentions.

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité / page vie privée sur votre site internet.

À l'issue de cette étape, vous avez répondu à votre obligation de transparence.

Permettez aux personnes d'exercer facilement leurs droits

Les personnes dont vous traitez les données (élèves, parents d'élèves, enseignants, etc.) ont des droits sur leurs données, qui sont d'ailleurs renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.
Vous devez leur donner les moyens d'exercer effectivement leurs droits. Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée.
Mettez en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

Pour en savoir plus :

- Exemples de mentions d'informations
- Respecter les droits des personnes

4ème étape	D. Sécurisez vos données

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données. Vous êtes en effet tenu à une obligation légale d'assurer la sécurité des données personnelles que vous détenez.

Vous garantissez ainsi l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.
Des réflexes doivent être mis en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- Les comptes utilisateurs sont-ils protégés par des mots de passe d'une complexité suffisante ?
- Les accès aux locaux sont-ils sécurisés ?
- Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

Pour en savoir plus :

- Guide des bonnes pratiques de l'informatique
- Guide de sécurité des données personnelles

9. Les documents de références :

- "Données numériques à caractère personnel au sein de l'éducation nationale", rapport n°2018-016, février 2018, IGEN, IGAENR, sous la direction de Gilles Braun et Jean-Marc Merriaux.
- "Les données à caractère personnel - Comprendre les nouvelles réglementations dans les établissements scolaires", CANOPE éditions, 2018.
- Le parcours M@gistère portant la mise en œuvre du cadre juridique du RGPD à l'École, disponible dans l'offre nationale en inscription libre.
- Protection des données personnelles : souriez, vous êtes traqués ! France Culture émission La Méthode scientifique par Nicolas Martin

10. Les ressources pédagogiques :

- La page de ressources éduscol dédiées à la mise en oeuvre du référentiel CNIL de formation des élèves à la protection des données personnelles.
- Arte propose pour Éduthèque un reportage dans les couloirs de l'Union européenne, Democracy : la ruée vers les datas, sur l'élaboration d'une législation pour la protection des données personnelles.
- disponible au téléchargement via éduthèque.
- Le site La mallette des parents propose les fiches suivantes :
    - La protection des données des enfants (partie "Parents")
      L'école a besoin de données indispensables sur votre enfant dans le cadre de sa scolarité. Le nouveau règlement européen sur la protection des données offre un cadre protecteur pour les citoyens. Vous êtes systématiquement informé de tout traitement de données à caractère personnel.
    - La protection des données personnelles à l'École (partie "Professionnels de l'éducation nationale")
      Lors de différentes réunions avec les parents, la question de la protection des données personnelles peut être abordée tant sur le suivi administratif et pédagogique de l'élève que par celui de l'éducation aux médias et à l'information (EMI).
- "C'est quoi la protection des données", 1 jour 1 question.
- "Protéger sa vie privée", Le rire jaune.
- Parcours EMI Les traces de DenisWeiss
- "Connais-moi, échappe-toi" un jeu d'évasion autour des données personnelles né d'une collaboration entre le CLEMI et la Délégation Académique au Numérique Éducatif (DANE) de l'académie de Besançon.
- Kit d'apprentissage sur la protection des données édité par Consumer Classroom, site multilingue, financé par la Commission européenne.
- Contrôle tes données dossier sur le site de la Quadrature du Net
- La protection des données personnelles sur Internet support de cours de Denis Szalkowski
- Sécurité des données personnelles : un guide pour agir et un test pour s'évaluer Sur EduScol, présentation du nouveau guide de la CNIL « sécurité » destiné à aider les responsables d'organismes traitant des données à respecter leurs obligations en matière de sécurité des données personnelles
- Maîtriser mes données dossier de la CNIL
- L'Observatoire Mes datas et moi Portail créé par une mutuelle d'assurances, la MAIF pour informer sur les risques liés aux données personnelles et aux comportements sur internet.
- GDPR / RGPD expliqué en emojis Vidéo sur You Tube par Cookie connecté
- Une cartographie des outils et pratiques de protection de la vie privée LINC - Laboratoire d'Innovation Numérique de la CNIL - publie sa cartographie d'exploration des outils et pratiques de protection de la vie privée, classées selon les usages et actions que chacun peut effectuer en ligne.
- Ne manquez pas la vidéo de l'Esprit sorcier sur la protection des données personnelles ! La CNIL a réalisé une vidéo avec Frédéric Courant, l'ancien animateur de l'émission « C'est pas Sorcier ». Objectif : mieux faire comprendre au public en quoi consiste la protection de ses données personnelles.
- La lettre Edu_Num Économie et gestion hors-série n°11 de janvier 2019 sur le thème de la protection des données personnelles dans les organisations.

11. Les interlocuteurs :

- Le **Délégué Académique à la Protection des Données** (DPD)
  Pierre Lafon
  Pierre.Lafon@ac-guyane.fr
  05 94 27 22 23

- La **Délégation Académique au Numérique Éducatif** (DANE),
  dane@ac-guyane.fr
  05 94 27 20 31